IN THE CLAIMS

1. - 50. (Canceled)

51. (Previously Presented) A machine-readable medium that provides instructions, which when executed by a wireless device, cause said machine to perform operations comprising:

selectively auditing a number of transactions between a wireless computing device and a server based on a type for the number of transactions, wherein selectively auditing of the number of transactions includes securely storing at least one attribute of selected audited transactions within the wireless computing device, wherein securely storing the at least one attribute of one of the selected audited transactions comprises:

storing at least one attribute of the selected audited transaction into an audit log into a memory in the wireless computing device;

encrypting the audit log based on an encryption key that is generated within the wireless computing device and wherein the encryption key is stored within a memory within a cryptographic processing module of the wireless computing device;

generating an integrity metric of the audit log; and

generating a signature of the integrity metric with a signature key that is generated and stored within the wireless computing device

incrementing an audit counter; and

storing a value of the audit counter, the integrity metric and the signature in the audit log

storing the encrypted audit log in a memory of a cryptographic processing module in the wireless computing device which performed the encrypting, in response to a determination that an audit session that includes the number of audit transactions is a high-valued audit session; and

storing the encrypted audit log in a memory that is external to the cryptographic processing module, in response to a determination that the audit session is not a high-value audit session.

52. (Previously Presented) The machine-readable medium of claim 51, wherein the at least one attribute is selected from a group consisting of the type of transaction, a monetary amount of the transaction and a time of the transaction.

53. (Previously Presented) The machine-readable medium of claim 51, wherein selectively auditing of the number of transactions includes opening an audit session upon receipt of one of the selected audited transactions, wherein securely storing the at least one attribute of one of the selected audited transactions includes storing at least one attribute of the selected audited transaction into an audit log into a memory in the wireless device.

54. (Previously Presented) The machine-readable medium of claim 53, wherein selectively auditing of the number of transactions further comprises:

closing the audit session; and

generating a hash of the audit log after the audit session is closed.

55. (New) A method comprising:

selectively auditing a number of transactions between a wireless computing device and a server based on a type for the number of transactions, wherein selectively auditing of the number of transactions includes securely storing at least one attribute of selected audited transactions within the wireless computing device, wherein securely storing the at least one attribute of one of the selected audited transactions comprises:

storing at least one attribute of the selected audited transaction into an audit log into a memory in the wireless computing device;

encrypting the audit log based on an encryption key that is generated within the wireless computing device and wherein the encryption key is stored within a memory within a cryptographic processing module of the wireless computing device;

generating an integrity metric of the audit log; and

generating a signature of the integrity metric with a signature key that is generated and stored within the wireless computing device incrementing an audit counter; and

storing a value of the audit counter, the integrity metric and the signature in the audit log

storing the encrypted audit log in a memory of a cryptographic processing module in the wireless computing device which performed the encrypting, in response to a determination that an audit session that includes the number of audit transactions is a high-valued audit session; and

storing the encrypted audit log in a memory that is external to the cryptographic processing module, in response to a determination that the audit session is not a high-value audit session.

56. (New) The method of claim 55, wherein the at least one attribute is selected from a group consisting of the type of transaction, a monetary amount of the transaction and a time of the transaction.

57. (New) The method of claim 55, wherein selectively auditing of the number of transactions includes opening an audit session upon receipt of one of the selected audited transactions, wherein securely storing the at least one attribute of one of the selected audited transactions includes storing at least one attribute of the selected audited transaction into an audit log into a memory in the wireless device.

58. (New) The method of claim 57, wherein selectively auditing of the number of transactions further comprises:

closing the audit session; and

generating a hash of the audit log after the audit session is closed.